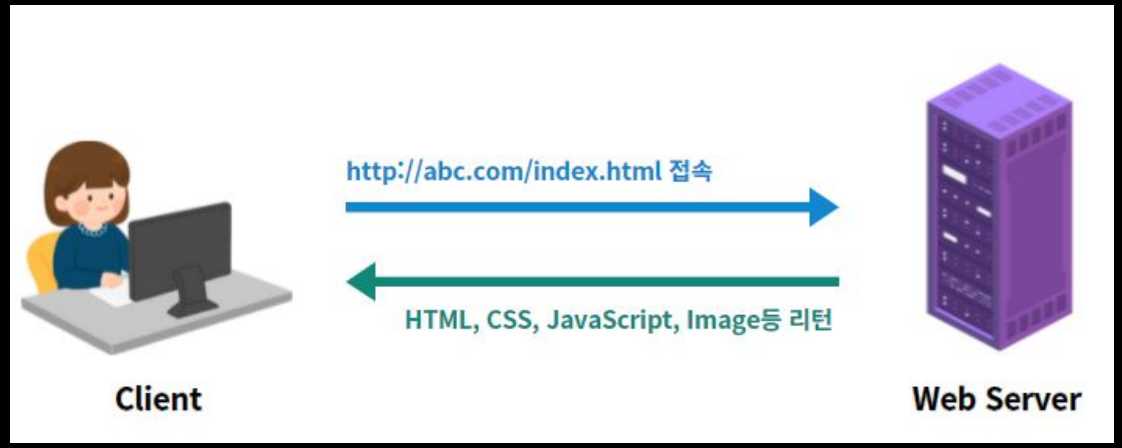
인공지능 보안

-12-

HTTP

HTTP (HyperText Transfer Protocol)

- 웹에서 가장 많이 쓰이는 프로토콜은 HTTP
- HTTP는 웹 처리 전반에 걸친 토대가 되기 때문에 웹 서버를 HTTP 서버라고 부르기도 함

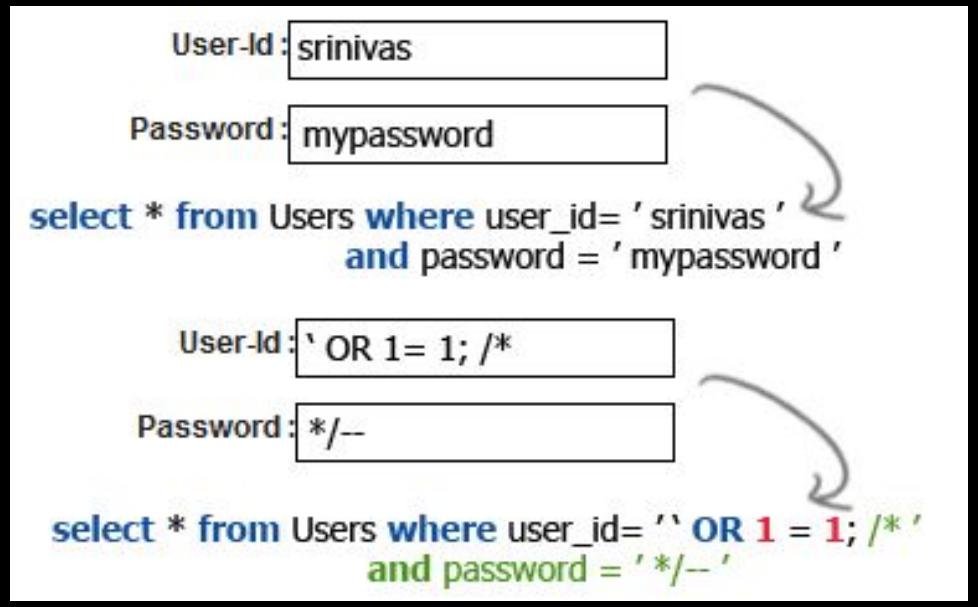


- 연결 과정
  - 클라이언트는 읽고자 하는 문서를 서버에 요청
  - 서버는 웹 문서 중에서 요청받은 것을 클라이언트에 전송

웹 서비스 취약점 공격

SQL Injection

악의적인 SQL문을 실행되게 함으로써 데이터베이스를 조작

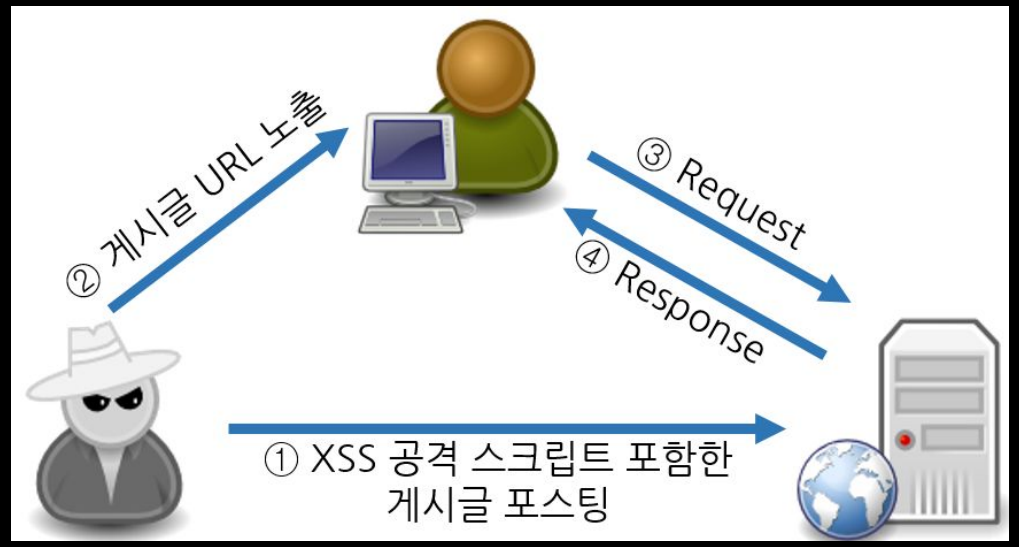


사용자의 입력이 SQL문에 동적으로 영향을 주는 경우, 입력된 값이 개발자가 의도한 값인지 검증하고 차단

/*, -, ‘, “, ?, #, (,), ;, @, =, *, +, union, select, drop, update, from, where, join, substr, user_tables, user_table_columns, information_schema, sysobject, table_schema, declare, dual,…

XSS (Cross Site Scripting)

웹 페이지에 악성 스크립트를 삽입하는 방식으로 이루어지는 공격
쿠키, 세션ID 탈취, 악성 코드 다운로드 등



스크립트 태그에 자주 사용되는 <, > 등 과 같은 문자를 필터링 해주는 방법으로 방어

랜섬웨어

랜섬웨어

- Ransomware = Ransom + Software
- 파일을 인질로 잡아 몸값을 요구하는 소프트웨어

랜섬웨어

- 공격자 입장에서 전세계 모든 인터넷 기기가 고객이 되어 지속적인 수익 창출 가능
- 가상화폐를 이용하여 추적이 불가능하고 공격 구조가 단순
- 몸값 지불시, 대부분 복구 ← 신뢰가 중요

랜섬웨어

- 기존 악성코드와의 차이
  - 정보를 유출하지 않음. 대신 정보를 암호화하여 접근하지 못하게 함.
  - 자기 자신을 숨기려고 하지 않음. 암호화 작업 후 금전적 대가 요구.
  - 악성코드 생성이 쉬움. 이미 공개되어 있는 강력한 암호화 알고리즘(RSA, AES 등)을 사용

랜섬웨어

- 방어 / 대응 방법


랜섬웨어 공격 프로세스
1 포털 및 SNS 접속
2 악성코드 다운로드
3 랜섬웨어 동작
4 문서 파일 등 검색
5 암호화 수행
6 결제 유도
1 악성 및 의심스런 웹 사이트 접속 차단
2 네트워크 레벨 악성코드 분석 및 차단
3 의심 파일 실행 감지 및 차단
4 반복적인 파일 검색 등 의심 행위 감지 및 차단
5 다량의 파일 암호화 등 의심 행위 감지 및 차단
6 결제 유도 등 의심 행위 감지 및 차단
이상적인 랜섬웨어 '실시간 대응' 프로세스 (보안기술 활용 관점)

Q&A